

EXHIBIT A

UNITED STATES DISTRICT COURT

for the
Eastern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 21-M-1318

Information associated with the accounts (1) "SARGENT GRAY" (FACEBOOK USER ID #
100069340365431); (2) "NECROPEDOCELL" (INSTAGRAM ACCOUNT ID # 45639960293)
and (3) Instagram Account "STAIN_LORD_352"
that is stored at premises controlled by Facebook, Inc)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before December 2, 2021 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .

Date and time issued: November 18, 2021 @1:28 p.m.

Marcia M. Henry
Judge's signature

City and state: Brooklyn, New York

Hon. Marcia M. Henry
James B. Cho U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

ReturnCase No.:
21-M-1318

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
*Printed name and title***Print****Save As...****Reset**

ATTACHMENT A

Property to be searched

This warrant applies to information associated with:

- “SARGENT GRAY” (FACEBOOK ID # 100069340365431)
- “NECROPEDOCELL” (INSTAGRAM ID # 45639960293) (active on, but not limited to, February 20, 2021)
- Instagram Account with Name “STAIN_LORD_352” (active on, but not limited to, November 2, 2021)

that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc., a company headquartered at 1601 Willow Road, Menlo Park, California

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by Facebook, Inc. (“Facebook”):

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Facebook, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A, from January 1, 2021 to the present:

- a. All business records and subscriber information, in any form kept, pertaining to the accounts, including:
 1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 2. All Facebook and Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 4. Devices used to login to or access the accounts, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 6. Internet Protocol (“IP”) addresses used to create, login, and use the accounts, including associated dates, times, and port numbers;
 7. Privacy and account settings, including change history; and

8. Communications between Facebook and any person regarding the accounts, including contacts with support services and records of actions taken;
- b. All content (whether created, uploaded, or shared by or with the accounts), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata;
- c. All content, records, and other information relating to communications sent from or received by the accounts, including but not limited to:
 1. The content of all communications sent from or received by the accounts, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
 2. All records and other information about direct, group, and disappearing messages sent from or received by the accounts, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
 3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
 4. All associated logs and metadata;
- d. All content, records, and other information relating to all other interactions between the accounts and other Facebook and Instagram users, including but not limited to:
 1. Interactions by other Facebook and Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
 2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
 3. All contacts and related sync information; and
 4. All associated logs and metadata;

- e. All records of searches performed by the account; and
- f. All location information, including location history, login activity, information geotags, and related metadata.

Facebook is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review all information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of: Title 18, United States Code, Sections 922(g)(1) (unlawful firearms possession by a convicted felon), 2252A (receipt, distribution, and possession of child pornography) and 48 (distribution of animal crush video) (the “Subject Offenses”), those violations involving Angel Almeida, occurring on or after January 1, 2021, including but not limited to:

- a. Documents and other records related to the acquisition or possession of firearms or ammunition;
- b. Documents and other records reflecting evidence of the receipt, distribution or possession of child pornography;
- c. Documents and other records reflecting evidence of “animal crushing” or “animal crush videos.”
- d. Documents and other records pertaining to any conspiracy, attempt or aiding and abetting the violation of the Subject Offenses.
- e. Evidence indicating the state of mind of the person who created, edited or used the data contained in the accounts;
- f. Documents and other records related to the locations where the Subject Offenses occurred;
- g. Records of or information about Internet Protocol addresses associated with access to the accounts;
- h. Evidence of user attribution showing who used or owned the accounts at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
- i. Contextual information necessary to understand the evidence described in this attachment.
- j. The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AAS:CRH
F. #2021R01035

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
ACCOUNTS:

- (1) “SARGENT GRAY” (FACEBOOK
USER ID # 100069340365431)
- (2) “NECROPEDOCELL” (INSTAGRAM
ACCOUNT ID # 45639960293)
- (3) Instagram Account
“STAIN_LORD_352”

THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK, INC.

TO BE FILED UNDER SEAL

**APPLICATION FOR SEARCH
WARRANTS FOR INFORMATION IN
POSSESSION OF A PROVIDER**

Case No. 21-M-1318

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, SEAN JOHNSON, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrant for information associated with the following accounts:

- (1) “SARGENT GRAY,” FACEBOOK ID # 100069340365431 (the “SARGENT ACCOUNT”)
- (2) “NECROPEDOCELL,” INSTAGRAM ID # 45639960293 (the “NECRO ACCOUNT”)
- (3) Instagram Account with name “STAIN_LORD_352,” (the “STAIN ACCOUNT”)

(together the “SUBJECT ACCOUNTS”), that is stored at premises controlled by Facebook, Inc. (“Facebook” or the “Provider”) a social media company located in Menlo Park, California.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18

U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (“FBI”). I have been a Special Agent with the FBI since 2017, and currently work on the FBI’s Joint Terrorism Task Force (“JTTF”) on matters related to domestic terrorism and violent extremism. As part of my duties, I investigate criminal violations relating to various federal crimes, including investigations into firearms. I have participated in the execution of search warrants, including searches of email and social media accounts, physical premises and electronic devices.

4. I am familiar with the facts and circumstances set forth below from my participation in the investigation and from reports of other law enforcement officers involved in the investigation.

5. The facts in this affidavit come from my personal observations, my training and experience, information obtained from both government and public records databases, information obtained from other agents and foreign law enforcement authorities, and review of records and documents. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

6. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, fruits and/or instrumentalities of violations of the Subject Offenses (as defined below), as described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

THE SUBJECT OFFENSES

8. For the reasons detailed below, I submit that there is probable cause to believe that the SUBJECT ACCOUNTS possess evidence, fruits, and/or instrumentalities of Title 18, United States Code, Sections 922(g)(1) (unlawful firearms possession by a convicted felon), 2252A (receipt, distribution, and possession of child pornography) and 48 (distribution of animal crush video) (the “Subject Offenses”), as more fully described in Attachment B.

PROBABLE CAUSE

9. In or around September 2021 and October 2021, the FBI received several tips regarding an individual named “Angel Almeida,” who, according to the tips, possessed firearms, was violent, and posted sexually explicit images of children online.

10. Specifically, on or about September 22, 2021, an individual identifying himself/herself only by first name contacted the FBI and wrote, in sum an substance and pertinent part, that Almeida (i) posts pictures of children in bondage wear, (ii) threatens to kill/sacrifice and

rape people; (iii) has met up with 16 year old and may have targeted other potential victims; and (iv) is a very dangerous individual.¹ The tipster identified certain social media profiles as used by Almeida, including the SARGENT ACCOUNT, among others. This tipster also stated that Almeida lives in Queens, New York.

11. On or about October 16, 2021, an anonymous individual wrote to the FBI:

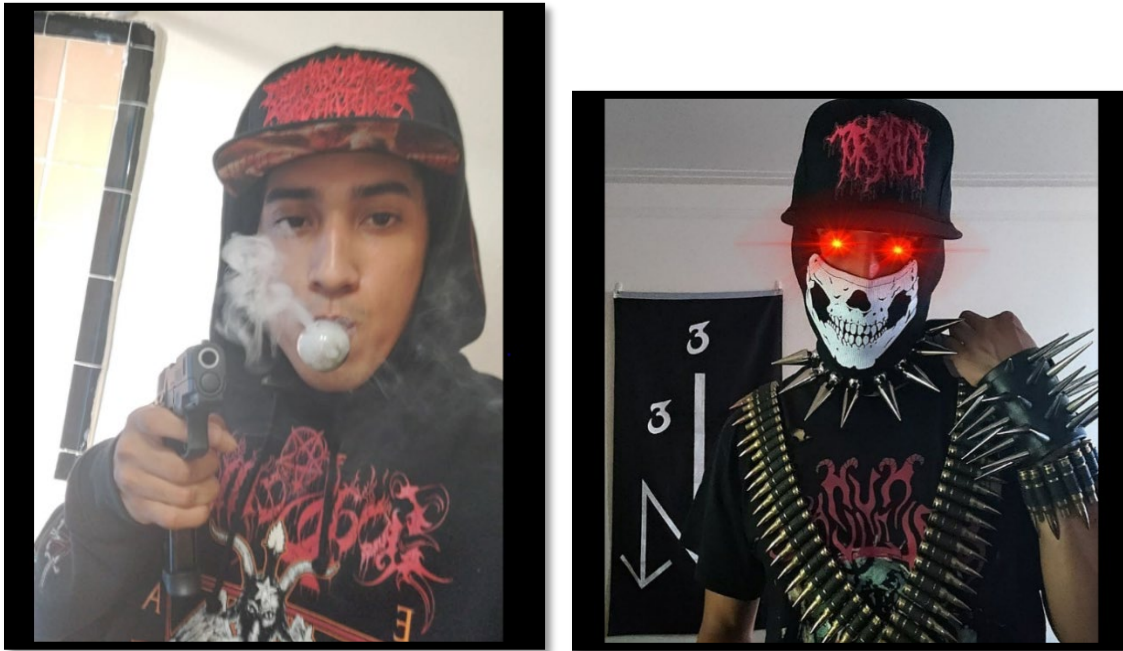
Angel Almeida (approximately age 21) originally from Ocala, FL with a previous record for Grand theft auto . . . sent child pornography to a minor. He is in possession of drugs and illegal guns (illegal due to his criminal record). He's incredibly dangerous and has stated he will "commit a kamakazi" if he doesn't hit his goal around age 25. He was recently seen around 985 Simpson Street Apartment 2H, Bronx, NY and believed to be residing with a family member. He consistently posts animal abuse material and has even posted images of himself having abused an animal by chopping it in half. He is extremely dangerous. He openly admits what he wants to do to children, posts his drug use online, and even posts child abuse material. His account will most likely be gone soon since his accounts do not last long but please look into this individual some of the images he had posted on previous accounts contained completely nude children. He will hurt someone if he hasn't already. A previous alias of his was also "necropedo".

The SARGENT ACCOUNT

12. According to records obtained from Facebook, the SARGENT ACCOUNT was created on June 13, 2021.

13. During my review of the publicly available portions of the SARGET ACCOUNT, I found the below photographs depicting an individual (who, for the reasons discussed below, I believe to be Almeida) with what appears to be a firearm and ammunition. The Facebook website indicates that these photographs were posted on August 13, 2021 (left) and July 20, 2021 (right), respectively.

¹ The FBI attempt to contact this individual have been unsuccessful.



14. Based on my training, experience, and open-source research, I know that the black flag in the background of Almeida's photograph is associated with the "Order of Nine Angles" or "O9A," a worldwide Satanist belief-based group which embraces elements of neo-Nazism and white supremacy. Members and associates of O9A have espoused violent, neo-Nazi, anti-Semitic, and Satanic beliefs, and have expressed admiration for figures such as Adolf Hitler and Usama Bin Laden. Members and associates of O9A have also participated in acts of violence, including murders.

15. Florida state criminal records indicate that, on or about February 27, 2019, "Angel Luis Almeida" was convicted of, among other things, burglary in the third degree, in violation of Florida Statute 810.02, a crime punishable by up to 5 years' imprisonment. That same day, Almeida was sentenced to serve 18 months' imprisonment. Florida prison records reflect that Almeida was released from prison on or about March 1, 2020. Based on a comparison of the above

photographs from the Facebook Account to a Florida arrest photograph of Angel Almeida, I believe that the photographs in the Facebook Account depict Almeida.

16. According to records from Amazon, on or about June 19, 2021, Angel Almeida purchased an item with the name “Nuoxinus Black Balaclava Ghosts Skull Full Face Mask for Cosplay Party Halloween Outdoor Motorcycle Bike Cycling Skateboard Hiking Skiing Snowmobile Snowboard” (the “Skull Mask”). Amazon shipped the item to an address in Queens, New York. An item for sale on Amazon matching that description is reflected immediately below:



17. Notably, the Skull Mask purchased by Almeida on June 19, 2021 appears to be the same mask as the one worn in the picture posted to the SARGENT ACCOUNT, which was posted one month later.

The NECRO ACCOUNT

18. According to records obtained from Facebook, the NECRO ACCOUNT was created on January 18, 2021.

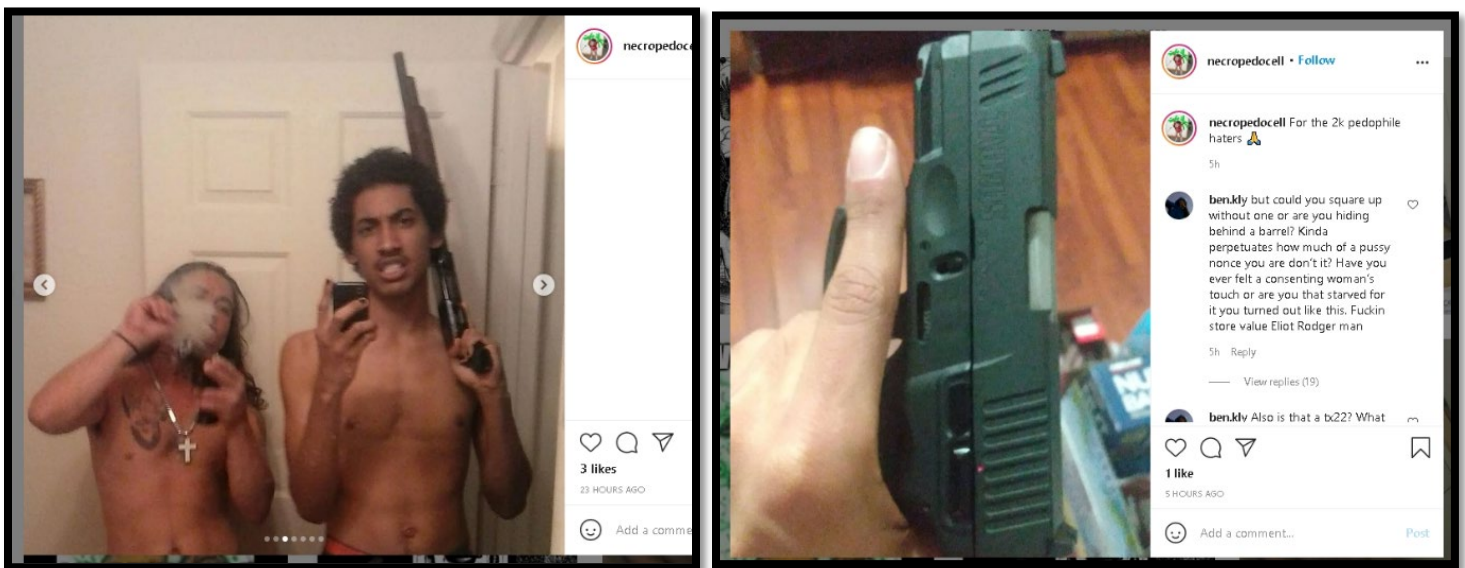
19. According to records from Facebook, a phone number ending in 7241 (the “7241 Phone”) was the verified² registered number for the NECRO ACCOUNT.

20. According to records provided by T-Mobile, “Angel Almeida” was the subscriber of the 7241 Phone in February 2021. According to T-Mobile records, Almeida resided in Queens, New York as of that date.

21. Based on my review of public portions of the NECRO ACCOUNT, I have found the following:

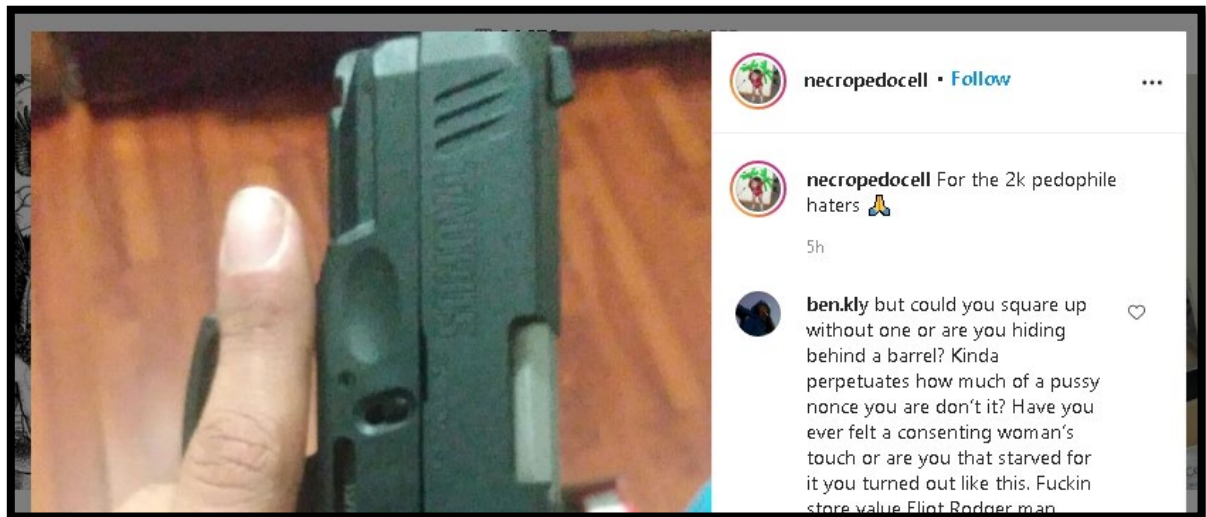
a. Multiple photographs of an individual who is identifiable as Almeida based on a comparison to other known photographs of Almeida.

b. Photographs of Almeida possessing firearms, including those posted on or about February 20, 2021 (left) and on or about February 20, 2021 (right).



² According to Instagram records, “Verified” indicates that the account holder responded to a text sent to the listed phone number.”

c. In certain of the posts on the NECRO ACCOUNT, Almeida expressed interest in and posts photographs consistent with violence against and sexual exploitation of minors. In a post on or about February 21, 2021, Almeida wrote, to accompany a photograph of a firearm, “For the 2k pedophile haters [preying hands emoji].”³



d. Similarly, on or about February 20, 2021, Almeida posted what appears, in my training and experience, to be a child, gagged and bound. Accompanying the photograph, Almeida wrote, “Life’s always been shit still I see the past through rose colored lenses.”

The STAIN ACCOUNT

22. I have also reviewed the publicly accessible portions of the STAIN ACCOUNT. From that review, I learned that Almeida acknowledged that the account belonged to him, admitted to owning and took pictures with a firearm, posted pictures depicting violence

³ Unless otherwise indicated, all text of postings described herein are reproduced with original spelling and grammar.

against animals, and threatened violence against police if they attempted to apprehend him. In particular:

a. On or about November 2, 2021, Almeida posted on the Stain Lord Account a photograph of a masked individual holding a firearm with the same mask and Order of Nine Angles flag depicted in photographs on the SARGENT ACCOUNT, which also appears to be the same mask that Almeida purchased from Amazon in June 2021.



b. On or about November 7, 2021, Almeida posted a photograph of Dylann Roof. Based on my training, experience, and open-source research, I know that Dylann Roof is a white supremacist who perpetrated a 2015 mass shooting at a Charleston church killing nine African Americans.

c. On or about November 13, 2021, Almeida posted a video of Elliot Rodger. Accompanying the video, Almeida wrote “My life story”. Based on my training, experience, and open-source research, I know that in 2014 Elliot Rodger killed six people and wounded 14 others in Isla Vista, California.

d. On or about November 9, 2021, Almeida posted the statement “Mfs be like ‘why you got a gun? It’s like you want to go back’” In response, someone wrote “They gonna Bobby smurda you boi” to which Almeida replied “not without a fight but shit regardless it’ll end my pain so idgaf.” Based on my training, experience, and open-source research, I know that Bobby Smurda is the stage name of a rapper who was convicted of a weapons charge in New York State court and that “idgaf” is an abbreviation for “I don’t give a fuck.”

e. On or about November 10, 2021, Almeida posted “People always testing my patience but who the fuck wants to link I’ll give you my addy or you can drop yours idgaf my name is Angel Luis Alméida see me about it or shut the fuck up.”

f. On or about November 13, 2021, Almeida posted a photograph of a bloody cat that had apparently been stabbed with a knife, along with the caption, “No limits evil,” and also posted a still from a video of a gun pointed at a dog with the caption, “bringing this classic back bcuz I’m getting to much followers and I don’t want soft cocks orbiting.”

g. On or about November 12, 2021, Almeida posted the below photograph of himself with appears to be a firearm.



h. On or about November 13, 2021, Almeida posted the below photograph of an individual standing in front of a Nazi flag with a shirt reading “Kiddie Fiddler” in front of a sign that reads, “I’M ADDICTED TO HARDCORE CHILD PORNOGRAPHY.”



23. Additionally, on or about November 14, 2021, an FBI employee acting in an undercover capacity online obtained the below photographs from a Telegram channel called “Rape Cast.” The photographs were posted anonymously.





24. Based on my review of the SARGENT ACCOUNT, the NECRO ACCOUNT, and the STAIN ACCOUNT, these photographs appear to be consistent with previous photographs Almeida has posted. The top photographs appear to contain the same mask and Order of Nine Angles flag previously referenced.

25. As the evidence above reflects, there is probable cause to believe that the SUBJECT ACCOUNTS contain evidence of the Subject Offenses, including evidence of the possession of firearms by a convicted felon, evidence of the possession of child pornography, evidence establishing Almeida's ongoing use of the SUBJECT ACCOUNTS, and evidence of Almeida's current whereabouts.

BACKGROUND ON FACEBOOK

26. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

27. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

28. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

29. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

30. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

31. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

32. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through

Facebook Messenger. These chat communications are stored in the chat history for the account.

Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

33. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

34. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

35. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

36. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

37. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

38. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a

Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

39. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

40. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

41. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained

by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

42. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning

subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

BACKGROUND ON INSTAGRAM

43. Instagram is a service owned by Facebook, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account listed in Attachment A-4, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

44. Facebook collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Facebook keeps records of changes made to this information.

45. Facebook also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

46. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the

primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

47. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Facebook maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

48. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

49. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Facebook to access the contact lists on their devices to identify which contacts are Instagram users. Facebook retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can

similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

50. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography (“Bio”), and a website address.

51. One of Instagram’s primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users (“tag”), or add a location. These appear as posts on the user’s profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Facebook’s servers.

52. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can “mention” others by adding their username to a comment preceded by “@”). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

53. An Instagram “story” is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain on Facebook’s servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

54. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

55. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

56. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

57. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily

searchable and can be “followed” to generate related updates from Instagram. Facebook retains records of a user’s search history and followed hashtags.

58. Facebook collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

59. Facebook uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Facebook maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user’s identity and activities, and it can also reveal potential sources of additional evidence.

60. In some cases, Instagram users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

61. For each Instagram user, Facebook collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

62. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

63. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

64. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Facebook can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

65. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

66. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, apps associated with the Instagram account may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

67. Therefore, Facebook's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

68. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require the Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

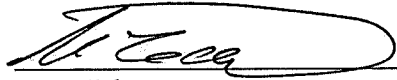
69. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING AND NON-DISCLOSURE

70. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the subjects of the investigation an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, notify confederates or otherwise seriously jeopardize the investigation. In this regard, I note that several of the subjects of this investigation are believed to be located overseas, in particular in Lebanon, a country from which extradition is difficult (if not impossible given the nature of this investigation). Some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the warrant, there is reason to believe that the subjects under investigation may destroy that evidence and change their patterns of behavior.

71. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue Orders commanding the Providers not to notify any person (including subscribers or customers of the accounts listed in the warrant) of the existence of the warrant for the period of one year from the date of the Order, except that Providers may disclose the warrant to its attorney(s) for the purpose of receiving legal advice.

Respectfully submitted,

 4/10/21
Sean Johnson
Special Agent
Federal Bureau of Investigation

Sworn to before me by telephone this
18th day of November, 2021

Marcia M. Henry
THE HONORABLE MARCIA M. HENRY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to be searched

This warrant applies to information associated with:

- “SARGENT GRAY” (FACEBOOK ID # 100069340365431)
- “NECROPEDOCELL” (INSTAGRAM ID # 45639960293) (active on, but not limited to, February 20, 2021)
- Instagram Account with Name “STAIN_LORD_352” (active on, but not limited to, November 2, 2021)

that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc., a company headquartered at 1601 Willow Road, Menlo Park, California

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by Facebook, Inc. (“Facebook”):

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Facebook, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A, from January 1, 2021 to the present:

- a. All business records and subscriber information, in any form kept, pertaining to the accounts, including:
 1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 2. All Facebook and Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 4. Devices used to login to or access the accounts, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 6. Internet Protocol (“IP”) addresses used to create, login, and use the accounts, including associated dates, times, and port numbers;
 7. Privacy and account settings, including change history; and

8. Communications between Facebook and any person regarding the accounts, including contacts with support services and records of actions taken;
- b. All content (whether created, uploaded, or shared by or with the accounts), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata;
- c. All content, records, and other information relating to communications sent from or received by the accounts, including but not limited to:
 1. The content of all communications sent from or received by the accounts, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
 2. All records and other information about direct, group, and disappearing messages sent from or received by the accounts, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
 3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
 4. All associated logs and metadata;
- d. All content, records, and other information relating to all other interactions between the accounts and other Facebook and Instagram users, including but not limited to:
 1. Interactions by other Facebook and Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
 2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
 3. All contacts and related sync information; and
 4. All associated logs and metadata;

- e. All records of searches performed by the account; and
- f. All location information, including location history, login activity, information geotags, and related metadata.

Facebook is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review all information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of: Title 18, United States Code, Sections 922(g)(1) (unlawful firearms possession by a convicted felon), 2252A (receipt, distribution, and possession of child pornography) and 48 (distribution of animal crush video) (the “Subject Offenses”), those violations involving Angel Almeida, occurring on or after January 1, 2021, including but not limited to:

- a. Documents and other records related to the acquisition or possession of firearms or ammunition;
- b. Documents and other records reflecting evidence of the receipt, distribution or possession of child pornography;
- c. Documents and other records reflecting evidence of “animal crushing” or “animal crush videos.”
- d. Documents and other records pertaining to any conspiracy, attempt or aiding and abetting the violation of the Subject Offenses.
- e. Evidence indicating the state of mind of the person who created, edited or used the data contained in the accounts;
- f. Documents and other records related to the locations where the Subject Offenses occurred;
- g. Records of or information about Internet Protocol addresses associated with access to the accounts;
- h. Evidence of user attribution showing who used or owned the accounts at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
- i. Contextual information necessary to understand the evidence described in this attachment.
- j. The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.